Some Gabidulin Codes Cannot be List Decoded Efficiently at any Radius

Netanel Raviv, *Student Member, IEEE,* and Antonia Wachter-Zeh, *Member, IEEE*

Abstract

Gabidulin codes can be seen as the rank-metric equivalent of Reed–Solomon codes. It was recently proven, using subspace polynomials, that Gabidulin codes cannot be list decoded beyond the so-called Johnson radius. In another result, cyclic subspace codes were constructed by inspecting the connection between subspaces and their subspace polynomials. In this paper, these subspace codes are used to prove two bounds on the list size in decoding certain Gabidulin codes. The first bound is an existential one, showing that exponentially-sized lists exist for codes with specific parameters. The second bound presents exponentially-sized lists explicitly, for a different set of parameters. Both bounds rule out the possibility of efficiently list decoding several families of Gabidulin codes for any radius beyond half the minimum distance. Such a result was known so far only for non-linear rank-metric codes, and not for Gabidulin codes. Using a standard operation called lifting, identical results also follow for an important class of constant dimension subspace codes.

Index Terms

Rank-metric codes, Gabidulin codes, list decoding, subspace polynomials, subspace codes.

I. Introduction

Rank-metric codes have recently attracted increasing interest due to their application to error correction in random network coding [30] where they can be used to construct constant dimension subspace codes. Further applications of codes in the rank metric include cryptography [11], [19], space-time coding [20], [21] and distributed storage systems [28], [29].

For a prime power q, let $\mathbb{F}_q$ be the field with q elements. For an integer n, let $\mathbb{F}_{q^n}$ be the extension field of degree n of $\mathbb{F}_q$ (which may be seen as the vector space of dimension n over $\mathbb{F}_q$, denoted by $\mathbb{F}_q^n$), and $\mathbb{F}_{q^n}^* \triangleq \mathbb{F}_{q^n} \setminus \{0\}$. For $m \geq n$, a rank-metric code is a set of $m \times n$ matrices over $\mathbb{F}_q$, or alternatively, a set of vectors of length n over the extension field $\mathbb{F}_{q^m}$, where the distance between two matrices is the rank of their difference. The *rate* of a rank metric code of size M is $\frac{\log_q M}{mn}$. *Gabidulin* codes, introduced by [6], [10], [27], may be seen as the rank-metric equivalent of Reed–Solomon codes. These codes are defined as evaluations of *linearized polynomials* (see below) of bounded degree at a given set of linearly independent evaluation points. We note that Gabidulin codes, and rank-metric codes in general, may be defined for any $m \geq n$, while our results only apply for the case n divides m (and in some cases, when $n+1$ divides m by puncturing). In particular, our results apply for $n = m$.

Given a word $w \in \mathbb{F}_{q^m}^n$ (or alternatively, a matrix $w \in \mathbb{F}_q^{m \times n}$), a *list decoding* algorithm outputs all Gabidulin codewords that are inside a ball of radius τ, centered at w, where τ is possibly larger than the unique decoding radius of the code. For a given code, a natural question to ask is: for which values of τ can list decoding be done efficiently? List decoding of rank-metric codes and Gabidulin codes was recently studied in [7], [15], [31]. In [31], it was shown that Gabidulin codes cannot be list decoded beyond the Johnson radius. This result was generalized to any rank-metric code by [7]. When m is sufficiently large, [7] also showed that with high probability a random rank-metric code can be efficiently list decoded. Further, it was shown in [31] that there is no Johnson-like polynomial upper bound on the list size since there exists a non-linear rank-metric code with exponentially growing list size for any radius greater than the unique decoding radius. In [15], an explicit subcode of a Gabidulin code was shown to be efficiently list decodable. In addition, [7], [15], and [31] have noted that it is not known if Gabidulin codes themselves can be efficiently list decoded beyond the unique decoding radius. In this paper, it is shown that the answer to this question is negative.

Clearly, if there exists a word $w \in \mathbb{F}_{q^m}^n$ with exponentially many Gabidulin codewords in a radius τ around it, then efficient list decoding is not possible for this radius. This combinatorial technique was used in [4] to show the limits of list decoding of Reed–Solomon codes, and in [31] to show the limits of list decoding of Gabidulin codes.

The main tool in [4], [31] is subspace polynomials, which are a special type of linearized polynomials. Linearized polynomials, defined by Ore [24], are polynomials of the form

$$P(x) = a_r \cdot x^{[r]} + \cdots + a_1 \cdot x^{[1]} + a_0 \cdot x,$$

The work of Netanel Raviv was supported in part by the Israeli Science Foundation (ISF), Jerusalem, Israel, under Grant no. 10/12, and by the IBM Ph.D. fellowship. The work of Antonia Wachter-Zeh was supported by a Minvera Postdoctoral Fellowship from the Max-Planck Society and by the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No 655109.

The authors are with the department of Computer Science, Technion – Israel Institute of Technology, Haifa 3200003, Israel (e-mail: {*netanel, antonia*}*@cs.technion.ac.il).*

Parts of this work have been presented at the *IEEE International Symposium on Information Theory (ISIT) 2015, HongKong, China* [25].

where $[i] \triangleq q^i$ and the coefficients are in the finite field $\mathbb{F}_{q^n}$ for some given n. For a linearized polynomial P, define the q-degree of P as $\deg_q P \triangleq r = \log_q \deg P$. Using the isomorphism between $\mathbb{F}_{q^n}$ and $\mathbb{F}_q^n$, every linearized polynomial may be seen as an $\mathbb{F}_q$-linear function from $\mathbb{F}_q^n$ to itself [18, Chapter 4, p. 108], that is, for every $\alpha, \beta \in \mathbb{F}_q$ and $u, v \in \mathbb{F}_{q^n}$, each linearized polynomial P satisfies $P(\alpha v + \beta u) = \alpha P(v) + \beta P(u)$. A subspace polynomial is defined as follows.

Definition 1. *[2]–[5], [31] A monic linearized polynomial P is called a subspace polynomial with respect to $\mathbb{F}_{q^n}$ if it satisfies the following equivalent conditions:*

A1. *P divides $x^{[n]} - x$.*
A2. *P splits completely over $\mathbb{F}_{q^n}$ and all its roots have multiplicity one.*
A3. *For some $0 \leq r \leq n$, there exists an r-dimensional subspace V of $\mathbb{F}_{q^n}$ such that $P(x) = \prod_{v \in V}(x - v)$.*

By A3, each subspace V corresponds to a unique subspace polynomial, denoted P_V. Subspace polynomials are an efficient method of representing subspaces, from which one can directly deduce certain properties of the subspace which are not evident in some other representations. These objects were studied in the past for various other purposes, e.g., construction of affine dispersers [3], finding an element of high multiplicative order in a finite field [5], and construction of cyclic subspace codes [2]. Albeit this wide range of applications, not much is known about the coefficients of subspace polynomials and their connection to the properties of the subspace.

It is known that all roots of every linearized polynomial have the same multiplicity, which is an integer power of q, and these roots form a subspace in the extension field [18, Theorem 3.50, p. 108]. Therefore, any monic linearized polynomial is a power of a subspace polynomial with respect to its splitting field. However, the structure of the coefficients of subspace polynomials, compared to other linearized polynomials of the same degree, is generally not known. A partial answer to this question was given by [2], and we use similar techniques to show limits of list decoding of Gabidulin codes.

Ben-Sasson et al. [4] proved that a given set of subspace polynomials with mutual top coefficients provides an upper bound on the list decoding radius of Reed–Solomon codes. A counting argument was later applied in order to show that such large sets of subspace polynomials do exist. A similar technique was used in [31] to show the limits of list decoding of Gabidulin codes. In the sequel, the existence of a set of subspaces whose polynomials have a larger agreement is proved (Theorem 3). This set is a subset of a subspace code by [2]. Furthermore, *explicit* dense sets of words in a Gabidulin code are provided (Theorem 4). Both bounds are used to show that the respective families of Gabidulin codes cannot be list decoded efficiently *at all*. That is, there exist received words that have exponentially many codewords around them, already for a radius which is only larger than the unique decoding radius by one (Examples 1 and 2, and Theorem 4). Due to a technical limitation of our techniques, the presented families have rate at least $\frac{1}{5}$.

Subspace codes have attracted an increasing interest recently due to their application in error correction in random network coding [17]. It is widely known that rank-metric codes are deeply connected to constant dimension subspace codes through an operation called lifting [12], [30]. This operation preserves the distance and the cardinality of the original rank-metric code. An important family of nearly optimal constant dimension subspace codes are *lifted Gabidulin codes* (that are a special case of the so-called Kötter and Kschischang codes [17]), which result from Gabidulin codes by lifting (see Definition 4). List decoding of subspace codes was extensively studied in recent years. In particular, several variants and subcodes of the Kötter and Kschischang codes were shown to be efficiently list decodable (e.g., [7], [15], [16], [22], [23] and references therein), and bounds equivalent to [31] were discussed in [26]. Our results about Gabidulin codes also apply for lifted Gabidulin codes, and thus we get families of subspace codes that cannot be list decoded efficiently at any radius. Our techniques may also be used for showing limits to list decoding of Reed–Solomon codes, but the resulting bounds are too weak to provide any useful insight.

These results reveal a significant difference in list decoding Gabidulin and Reed–Solomon codes, although the definitions of these code classes strongly resemble each other. Namely, Reed–Solomon codes can be efficiently list decoded up to the Johnson radius (with the Guruswami-Sudan algorithm [14]), whereas we have just proven that (some classes of) Gabidulin codes cannot be list decoded efficiently at all.

The rest of the paper is organized as follows. Notations for subspace codes and the subspace code from [2] will be described in Section II, together with the required background on cyclic shifts of subspaces and q-associates of polynomials. In Section III, the code from Section II is used to prove the existence of a certain set of subspace polynomials, and the notion of q-associates is used to show an explicit set of another type of subspace polynomials. The improved bounds on list decodability of Gabidulin codes are discussed in Section IV, implications about subspace codes are discussed in Section V, and conclusions are given in Section VI. A discussion about the inapplicability of our techniques to list decodability of Reed–Solomon codes appears in Appendix A.

II. Preliminaries

The set $\mathcal{G}_q(n, r)$, called the *Grassmannian*, is the set of all subspaces of dimension r (r-subspaces, in short) of $\mathbb{F}_{q^n}$. The size of $\mathcal{G}_q(n, r)$ is given by the Gaussian coefficient $\begin{bmatrix} n \\ r \end{bmatrix}_q \triangleq \prod_{i=0}^{r-1} \frac{q^{n-i}-1}{q^{i+1}-1}$, which satisfies $q^{r(n-r)} \leq \begin{bmatrix} n \\ r \end{bmatrix}_q \leq 4q^{r(n-r)}$ [12]. A constant dimension *subspace code* [17] is a subset of $\mathcal{G}_q(n, r)$ under the *subspace metric* $d_S(U, V) = \dim U + \dim V - 2\dim(U \cap V)$.

An extensively used concept in this paper is *cyclic shifts* of subspaces, defined as follows.

Definition 2. *For $V \in \mathcal{G}_q(n,r)$ and $\alpha \in \mathbb{F}_{q^n}^*$ let $\alpha V \triangleq \{\alpha v | v \in V\}$.*

The set αV, which is clearly a subspace of the same dimension as V, is called a *cyclic shift* of V. Cyclic shifts were shown to be useful for constructing subspace codes [2], [9]. The set of all cyclic shifts of $V \in \mathcal{G}_q(n,r)$ is called the *orbit* of V, and its size is $\frac{q^n-1}{q^t-1}$ for some integer t which divides n. The size of the orbit and the structure of its subspace polynomials can be derived by inspecting the subspace polynomial of V, as shown in the following lemmas.

Lemma 1. *[2, Lemma 5] If $V \in \mathcal{G}_q(n,r)$ and $\alpha \in \mathbb{F}_{q^n}^*$ then $P_{\alpha V}(x) = \alpha^{[r]} \cdot P_V(\alpha^{-1}x)$. That is, if $P_V(x) = x^{[r]} + \sum_{j=0}^{r-1} \alpha_j x^{[j]}$ then $P_{\alpha V}(x) = x^{[r]} + \sum_{j=0}^{r-1} \alpha^{[r]-[j]} \alpha_j x^{[j]}$.*

Lemma 2. *[2, Corollary 3] Let $V \in \mathcal{G}_q(n,r)$ and $P_V(x) = x^{[r]} + \sum_{j=0}^{r-1} \alpha_j x^{[j]}$. If $\alpha_s \neq 0$ for some $s \in \{1,\ldots,r-1\}$ and $\gcd(s,n) = t$, then V has at least $\frac{q^n-1}{q^t-1}$ distinct cyclic shifts.*

In [2] it is shown that subspaces in $\mathcal{G}_q(n,r)$, that may be considered as subspaces over a subfield of $\mathbb{F}_{q^n}$ which is larger than $\mathbb{F}_q$, admit a unique subspace polynomial structure. In what follows we cite the essentials from [2]. For an integer g such that $g | \gcd(n,r)$, let h be any $\mathbb{F}_{q^g}$ isomorphism between $\mathbb{F}_{q^g}^{n/g}$ and $\mathbb{F}_{q^n}$, and notice that for all $u, v \in \mathbb{F}_{q^g}^{n/g}$ and $\alpha, \beta \in \mathbb{F}_{q^g}$, we have that $h(\alpha v + \beta u) = \alpha h(v) + \beta h(u)$. For $V \in \mathcal{G}_{q^g}(n/g, r/g)$ let $H(V) \triangleq \{h(v) | v \in V\}$. The set $H(V)$ is clearly a subspace of dimension r over $\mathbb{F}_q$ in $\mathbb{F}_{q^n}$. Furthermore, the function $H : \mathcal{G}_{q^g}(n/g, r/g) \to \mathcal{G}_q(n,r)$ is injective since h is injective.

Construction 1. *[2, Construction 1] For integers $g, n,$ and r such that $0 < r < n$ and $g | \gcd(n,r)$, let*

$$\mathbb{C}_g \triangleq \{H(V) | V \in \mathcal{G}_{q^g}(n/g, r/g)\}.$$

Clearly, for $g = 1$ Construction 1 is trivial. Thus, we henceforth assume that $g \geq 2$, i.e., n and r have a non-trivial $\gcd$. The subspace code $\mathbb{C}_g$ has minimum subspace distance $2g$, and it may alternatively be defined as direct sums of cyclic shifts of $\mathbb{F}_{q^g}$ or as the set of all subspace of $\mathcal{G}_q(n,r)$ that are subspaces over $\mathbb{F}_{q^g}$ as well [2]. Since $\mathbb{C}_g$ is the image of an injective function from $\mathcal{G}_{q^g}(n/g, r/g)$ to $\mathcal{G}_q(n,r)$, we have the following.

Corollary 1. *[2, Corollary 5]* $|\mathbb{C}_g| = \begin{bmatrix} n/g \\ r/g \end{bmatrix}_{q^g}$.

The subspaces in $\mathbb{C}_g$ admit a unique subspace polynomial structure, from which the results in this paper follow.

Lemma 3. *[2, Lemma 14] If $V \in \mathcal{G}_q(n,r)$ then $V \in \mathbb{C}_g$ if and only if $P_V(x) = \sum_{i=0}^{r/g} c_i x^{[gi]}$, where $c_i \in \mathbb{F}_{q^n}, \forall i \in \{0,\ldots,r/g\}$.*

Another concept used in our constructions is the notion of q-associates. Two polynomials over $\mathbb{F}_{q^n}$ of the form $\ell(x) = \sum_{i=0}^{d} \alpha_i x^i$ and $L(x) = \sum_{i=0}^{d} \alpha_i x^{q^i}$, are called q-associates of each other. For any $g \in \mathbb{N}$, one can similarly define q^g-associativity, where $\ell(x) = \sum_{i=0}^{d} \alpha_i x^i$, and $L(x) = \sum_{i=0}^{d} \alpha_i x^{q^{gi}}$ are q^g-associates of each other. Linearized polynomials over $\mathbb{F}_q$ are deeply connected to their q-associates as follows.

Lemma 4. *[18, Theorem 3.62, p. 116] If $L_1(x)$ and $L(x)$ are linearized polynomials over $\mathbb{F}_q$ with q-associates $\ell_1(x)$ and $\ell(x)$, then $L_1(x)$ divides $L(x)$ if and only if $\ell_1(x)$ divides $\ell(x)$.*

III. Sets of Subspaces Polynomials with Mutual Top Coefficients

In [4] (resp. [31]) it was shown that sets of subspace polynomials that agree on many of their top coefficients provide a bound on the list decodability of Reed–Solomon (resp. Gabidulin) codes. By Lemma 3 it is evident that all subspace polynomials of subspaces in $\mathbb{C}_g$ agree on their topmost g coefficients $(1,0,\ldots,0)$. Using a counting argument we may prove the existence of a subset of $\mathbb{C}_g$ whose corresponding subspace polynomials agree on a larger number of top coefficients.

Theorem 1. *If $g, n,$ and r are integers such that $0 < r < n$, $g | \gcd(r,n)$, and ℓ is the unique non-negative integer such that $r = n - g(\ell+1)$, then there exists a subset of $\mathbb{C}_g$ of size at least*

$$\frac{\begin{bmatrix} n/g \\ r/g \end{bmatrix}_{q^g}}{q^{n\ell}},$$

whose subspace polynomials agree on their topmost $g(\ell+1)$ coefficients.

Proof: Consider the set of all subspace polynomials of subspaces in $\mathbb{C}_g$ (Construction 1). Lemma 3 implies that these polynomials have zero coefficients for all monomials $x^{[j]}$ such that $g \nmid j$. Hence, they may be partitioned into $q^{n\ell}$ subsets according to their $\ell+1$ top coefficients which correspond to monomials whose q-degree is divisible by g. According to the pigeonhole principle, there exists a subset of size at least $\begin{bmatrix} n/g \\ r/g \end{bmatrix}_{q^g} / q^{n\ell}$ whose polynomials agree on their top $g(\ell+1)$ coefficients. ∎

Notice that for $g = 1$, Theorem 1 reduces to the ordinary counting argument employed by [4] and [31]. In addition, the case where $n - r = g(\ell + 1) \geq r$, in which the polynomials in the set agree on *all* coefficients, is also trivial, since it merely implies the existence of a set of size one. Hence, this theorem is applicable only when $r > n/2$.

The notion of q^g-associativity, together with Lemma 1, allows us to construct an *explicit* large set of subspace polynomials. It will also be noted that in certain cases, this set of polynomials corresponds to the entire set $\mathbb{C}_g$. The construction is based on the following lemma.

Lemma 5. *If g, s, and r are integers such that $gs|r$ and $n \triangleq r+gs$, then the polynomial $P(x) \triangleq \sum_{i=0}^{n/gs-1} x^{[igs]}$ is a subspace polynomial with respect to $\mathbb{F}_{q^n}$.*

Proof: Since $gs|r$, there exists an integer α such that $gs\alpha = r$, thus $n = gs(\alpha+1)$ and $s|\frac{n}{g}$. It follows that

$$\frac{x^{n/g}-1}{x^s-1} = x^{\frac{n}{g}-s} + x^{\frac{n}{g}-2s} + \ldots + 1,$$

and hence $(x^{n/g-s} + x^{n/g-2s} + \ldots + 1)|(x^{n/g} - 1)$. According to Lemma 4, the q^g-associates of these polynomials satisfy $\sum_{i=0}^{n/gs-1} x^{[igs]}|(x^{[n]} - x)$, and thus P is a subspace polynomial of an r-subspace in $\mathbb{F}_{q^n}$ by Definition 1. ∎

By Lemma 1 and Lemma 5, we have a large set of subspace polynomials whose coefficients may be given explicitly.

Construction 2. *If g, s, and r are integers such that $gs|r$ and $n \triangleq r + gs$, then*

$$\mathcal{Z} \triangleq \left\{ \sum_{i=0}^{n/gs-1} \beta^{[r]-[igs]} x^{[igs]} \;\middle|\; \beta \in B \right\}$$

consists of $\frac{q^n-1}{q^{gs}-1}$ subspace polynomials of subspaces in $\mathcal{G}_q(n, r)$, where B is any set of nonzero representatives of the orbit of $\mathbb{F}_{q^{gs}}$.

Proof: Since $n = r + gs$ and $gs|r$, it follows that $gs|n$, and thus $\mathbb{F}_{q^{gs}}$ is a subfield of $\mathbb{F}_{q^n}$. By Lemma 5, the polynomial $P_V(x) = \sum_{i=0}^{n/gs-1} x^{[igs]}$ is a subspace polynomial of some $V \in \mathcal{G}_q(n, r)$. Let B be any set of representatives of the orbit of $\mathbb{F}_{q^{gs}}$, that is, a set consisting of a single nonzero element from each subspace in $\{\alpha\mathbb{F}_{q^{gs}} | \alpha \in \mathbb{F}_{q^n}^*\}$. Since the size of the orbit of $\mathbb{F}_{q^{gs}}$ is $\frac{q^n-1}{q^{gs}-1}$, and since all subspaces in it intersect trivially [9, Section III], it follows that $|B| = \frac{q^n-1}{q^{gs}-1}$. By Lemma 1, for all $\beta \in B$ we have that $P_{\beta V}(x) \in \mathcal{Z}$. We are left to show that if $\beta_1, \beta_2 \in B$, then $\beta_1 V \neq \beta_2 V$.

Assume for contradiction that there exists $\beta_1, \beta_2 \in B$ such that $\beta_1 V = \beta_2 V$. It follows that $P_{\beta_1 V}(x) = P_{\beta_2 V}(x)$, and Lemma 1 implies that the coefficients of x are equal, that is, $\beta_1^{[n-gs]-1} = \beta_2^{[n-gs]-1}$. Therefore, since every $\alpha \in \mathbb{F}_{q^n}$ satisfies $\alpha^{q^n} = \alpha$, we have that

$$\begin{aligned}
\left(\beta_1^{q^{n-gs}-1}\right)^{-q^{gs}} &= \left(\beta_2^{q^{n-gs}-1}\right)^{-q^{gs}} \\
\beta_1^{q^{gs}-q^n} &= \beta_2^{q^{gs}-q^n} \\
\beta_1^{q^{gs}-1} &= \beta_2^{q^{gs}-1} \\
\left(\frac{\beta_1}{\beta_2}\right)^{q^{gs}-1} &= 1.
\end{aligned}$$

It is widely known (e.g., [18, Theorem 3.20, p. 91]) that the subspace polynomial of $\mathbb{F}_{q^{gs}}$ is $x^{q^{gs}} - x$, which implies that $\beta_1\beta_2^{-1} \in \mathbb{F}_{q^{gs}}$, and thus $\beta_1 \in \beta_2\mathbb{F}_{q^{gs}}$. Since $\beta_2 \in \beta_2\mathbb{F}_{q^{gs}}$, it follows that β_1 and β_2 belong to the same cyclic shift $\beta_2\mathbb{F}_{q^{gs}}$, a contradiction. ∎

Notice that the set B of representatives of $\mathbb{F}_{q^{gs}}$ (see Construction 2) may easily be found. For example, if γ is a primitive element of $\mathbb{F}_{q^n}$, since the set $\{0\} \cup \{\gamma^{i(q^n-1)/(q^{gs}-1)}\}_{i=0}^{q^{gs}-2}$ is $\mathbb{F}_{q^{gs}}$, it follows that a possible set of representatives of the orbit of $\mathbb{F}_{q^{gs}}$ is

$$B \triangleq \left\{ \gamma^i \;\middle|\; 0 \leq i \leq \frac{q^n-1}{q^{gs}-1} - 1 \right\}.$$

Remark 1. *For $s = 1$, the set $\mathcal{Z}$ from Construction 2 consists of all subspace polynomials of subspaces in $\mathbb{C}_g$ (see Construction 1). This is since the number of cyclic shifts of $\mathbb{F}_{q^g}$ is $\frac{q^n-1}{q^g-1}$ and the size of $\mathbb{C}_g$ is $\begin{bmatrix} n/g \\ r/g \end{bmatrix}_{q^g} = \begin{bmatrix} n/g \\ n/g-1 \end{bmatrix}_{q^g} = \frac{q^n-1}{q^g-1}$.*

In Section IV, we consider subspace polynomials over $\mathbb{F}_{q^n}$ as polynomials over an extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_{q^n}$. In order to use the above claims over $\mathbb{F}_{q^m}$, the following formal lemma is required. The proof of this lemma is an immediate corollary of the existence of an injective homomorphism $\phi : \mathbb{F}_{q^n} \to \mathbb{F}_{q^m}$.

Lemma 6. *Let $P_V(x) = x^{[r]} + \sum_{j=0}^{r-1} v_j x^{[j]}$ and $P_U(x) = x^{[r]} + \sum_{j=0}^{r-1} u_j x^{[j]}$ be two subspace polynomials of subspaces in $\mathcal{G}_q(n,r)$, and let $\mathbb{F}_{q^m}$ be an extension field of $\mathbb{F}_{q^n}$. If we consider P_V, P_U as polynomials $P_{V'}, P_{U'}$ over $\mathbb{F}_{q^m}$, i.e.,*

$$P'_V(x) = x^{[r]} + \sum_{j=0}^{r-1} v'_j x^{[j]}$$

$$P'_U(x) = x^{[r]} + \sum_{j=0}^{r-1} u'_j x^{[j]}$$

where the coefficients are in $\mathbb{F}_{q^m}$, then for all $j \in \{0,\ldots,r-1\}$, $v_j = u_j$ if and only if $v'_j = u'_j$. Furthermore, the polynomials $P_{V'}, P_{U'}$ are subspace polynomials in $\mathcal{G}_q(m,r)$.

Notice that generalizing Lemma 6 to the case where $\mathbb{F}_{q^m}$ is not an extension field of $\mathbb{F}_{q^n}$, i.e. U and V are subspaces in $\mathbb{F}_{q^m}$ which are contained in a subspace of dimension n, is not clear. However, such a generalization is necessary to use our techniques to bound the list size for any $m \geq n$.

IV. Improved Bounds on List Decodability of Gabidulin Codes

We begin by formally defining Gabidulin codes, which are rank-metric codes that attain a *Singleton*-like bound. Any rank-metric code over $\mathbb{F}_{q^m}$ of length n, minimum rank distance d, and size M satisfies $M \leq q^{m(n-d+1)}$ [6], [27]. For a linear rank-metric code of dimension k, this bound implies that $d \leq n-k+1$. Codes which attain this bound are called *maximum rank distance* (MRD) codes. It can be shown that Gabidulin codes, defined below, are linear MRD codes, attaining $d = n-k+1$.

Definition 3. *[10] A linear Gabidulin code $\mathrm{Gab}[n,k]$ over $\mathbb{F}_{q^m}$, length $n \leq m$, and dimension $k \leq n$ is the set*

$$\mathrm{Gab}[n,k] \triangleq \left\{ (P(\alpha_1),\ldots,P(\alpha_n)) \,|\, \deg_q P < k \right\},$$

where P traverses all q-degree restricted linearized polynomials, and $\alpha_1,\ldots,\alpha_n$ are some fixed elements of $\mathbb{F}_{q^m}$ which are linearly independent over $\mathbb{F}_q$.

In [31] it was shown that large sets of subspace polynomials that agree on many top coefficients may be used to show the limits of list decoding of Gabidulin codes. For the lack of knowledge about the structure of the coefficients of subspace polynomials, a counting argument was later applied to show the existence of such a set. The resulting bound on list decoding of Gabidulin codes is cited below. In what follows, for $w \in \mathbb{F}_{q^m}^n$ and $\tau \in \mathbb{N}$, let $B_\tau(w) \triangleq \{c \,|\, \mathrm{rank}(w-c) \leq \tau\}$, that is, a ball of radius τ centered at w.

Theorem 2. *[31, Theorem 1] Consider the code $\mathrm{Gab}[n,k]$ over $\mathbb{F}_{q^m}$, with $d = n-k+1$. If $\tau < d$, then there exists a word $w \in \mathbb{F}_{q^m}^n$ such that*

$$|\mathrm{Gab}[n,k] \cap B_\tau(w)| \geq \frac{\begin{bmatrix} n \\ n-\tau \end{bmatrix}_q}{(q^m)^{n-\tau-k}}.$$

As a result, the following bound is achieved.

Corollary 2. *[31, Section III] The code $\mathrm{Gab}[n,k]$ over $\mathbb{F}_{q^m}$, with $d = n-k+1$ cannot be list decoded efficiently for any list decoding radius*

$$\tau \geq \frac{m+n}{2} - \sqrt{\frac{(m+n)^2}{4} - m(d-\varepsilon)},$$

for any fixed $0 \leq \varepsilon < 1$.

For $n = m$, this bound simplifies to

$$\tau \geq n - \sqrt{n(n-d+\varepsilon)},$$

which may be seen as the rank-metric equivalent of the Johnson radius [13], and for $\varepsilon = 0$ it is equal to the Hamming-metric Johnson radius.

By Lemma 3, in certain cases there exists a large set of subspace polynomials with a unique coefficient structure. Restricting the counting argument used in the proof of Theorem 2 to the set $\mathbb{C}_g$ (Theorem 1) provides a bound which may outperform Corollary 2. The proof of the following theorem is illustrated in Fig. 1, and its consequences are discussed in the sequel.

Theorem 3. *For integers $k \leq n \leq m$ such that n divides m, let $\mathrm{Gab}[n,k]$ be a linear Gabidulin code over $\mathbb{F}_{q^m}$, with $d = n-k+1$ and evaluation points $\alpha_1,\ldots,\alpha_n \in \beta\mathbb{F}_{q^n}$ for some $\beta \in \mathbb{F}_{q^m}^*$. Let τ, g be integers such that $\lfloor \frac{d-1}{2} \rfloor + 1 \leq \tau \leq d-1$,*

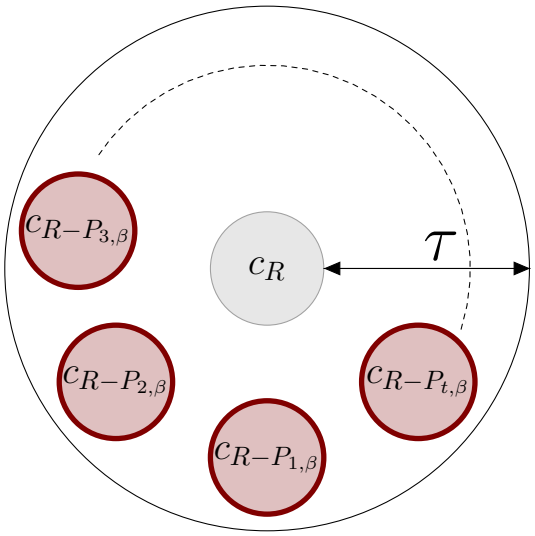

Fig. 1. An illustration of the proof of Theorem 3. The proof of Theorem 4 is similar. The ball around c_R of radius τ contains the words $c_{R-P_{i,\beta}}$ for $P_{i,\beta} \in \mathcal{P}_\beta$, where $|\mathcal{P}_\beta| = \begin{bmatrix} n/g \\ (n-\tau)/g \end{bmatrix}_{q^g} \Big/ q^{n\ell}$.

$g \geq 2$, and $g | \gcd(n-\tau, n)$. If ℓ is the unique integer such that $n = n - \tau + g(\ell+1)$ (and thus, $\tau = g(\ell+1)$), then there exists a word $c_R \in \mathbb{F}_{q^m}^n \setminus \mathrm{Gab}[n,k]$ such that

$$|\mathrm{Gab}[n,k] \cap B_\tau(c_R)| \geq \frac{\begin{bmatrix} n/g \\ (n-\tau)/g \end{bmatrix}_{q^g}}{q^{n\ell}}. \tag{1}$$

Proof: According to Theorem 1, there exists a set $\mathcal{P}$ of $\begin{bmatrix} n/g \\ (n-\tau)/g \end{bmatrix}_{q^g} / q^{n\ell}$ subspace polynomials of subspaces in $\mathcal{G}_q(n, n-\tau)$, that agree on their topmost $\tau = g(\ell+1)$ coefficients. The coefficients of these polynomials are in the field $\mathbb{F}_{q^n}$. Since $n|m$, we have that $\mathbb{F}_{q^n}$ is a subfield of $\mathbb{F}_{q^m}$, and thus these coefficients may be considered as elements of $\mathbb{F}_{q^m}$. Recall that according to Lemma 6, these polynomials agree on their topmost τ coefficients also when considered as polynomials over $\mathbb{F}_{q^m}$.

Further, let $\{V_P\}_{P \in \mathcal{P}} \subseteq \mathcal{G}_q(n, n-\tau)$ be the subspaces which correspond to the subspace polynomials in $\mathcal{P}$. For $P \in \mathcal{P}$, let P_β be the subspace polynomial of βV_P, and let $\mathcal{P}_\beta \triangleq \{P_\beta\}_{P \in \mathcal{P}}$. According to Lemma 1, and according to the properties of $\mathcal{P}$, it follows that the polynomials in $\mathcal{P}_\beta$ agree on their topmost τ coefficients. Since multiplication by β is an injection, it also follows that $|\mathcal{P}| = |\mathcal{P}_\beta|$.

Let R be any linearized polynomial over $\mathbb{F}_{q^m}$ of q-degree $n-\tau$ that has the mutual top coefficients of $\mathcal{P}_\beta$, and let $c_R \in \mathbb{F}_{q^m}^n$ be the word resulting from the evaluation of R at $\alpha_1, \ldots, \alpha_n$. Similarly, for $P_\beta \in \mathcal{P}_\beta$ let $c_{R-P_\beta} \in \mathbb{F}_{q^m}^n$ be the word corresponding to the evaluation of $R - P_\beta$ at $\alpha_1, \ldots, \alpha_n$.

Since $\deg_q(R - P_\beta) \leq n - \tau - g(\ell+1)$ and $\tau = g(\ell+1) > \frac{d-1}{2} = \frac{n-k}{2}$ it follows that $2\tau = \tau + g(\ell+1) > n - k$, and hence,

$$k > n - \tau - g(\ell+1) \geq \deg_q(R - P_\beta).$$

Therefore, the word c_{R-P_β} is a codeword of $\mathrm{Gab}[n,k]$ for all $P_\beta \in \mathcal{P}_\beta$. In addition, since $\tau \leq d-1$ it follows that $\deg_q R = n - \tau \geq n - d + 1 = k$, and hence $c_R \notin \mathrm{Gab}[n,k]$.

Since every linearized polynomial can be viewed as an $\mathbb{F}_q$-linear mapping (see Section I), it follows that for every $P_\beta \in \mathcal{P}_\beta$,

$$\begin{aligned} \mathrm{rank}(c_R - c_{R-P_\beta}) &= \mathrm{rank}((P_\beta(\alpha_1), \ldots, P_\beta(\alpha_n))) \\ &= \dim \langle P_\beta(\alpha_1), \ldots, P_\beta(\alpha_n) \rangle \\ &= \dim P_\beta(\langle \alpha_1, \ldots, \alpha_n \rangle) \\ &= \dim P_\beta(\beta \mathbb{F}_{q^n}), \end{aligned}$$

where the last equality follows from the fact that $\alpha_1, \ldots, \alpha_n$ are n linearly independent elements in $\beta\mathbb{F}_{q^n}$, a subspace of dimension n. Since P_β is a subspace polynomial of βV_P, which is a subspace of dimension $n-\tau$ that is contained in $\beta\mathbb{F}_{q^n}$, it follows that $\dim P_\beta(\beta\mathbb{F}_{q^n}) = \tau$. Thus, the set $\{c_{R-P_\beta}\}_{P_\beta \in \mathcal{P}_\beta} \subseteq \mathrm{Gab}[n,k]$ is a set of size $\begin{bmatrix} n/g \\ (n-\tau)/g \end{bmatrix}_{q^g} / q^{n\ell}$, which is contained in a ball of radius τ around the word c_R. ∎

Notice that the restriction on the parameter r, mentioned after the proof of Theorem 1, implies the necessary condition $r = n - \tau > n/2$, and hence $\tau < n/2$. However, this limitation becomes trivial when discussing τ which is approximately the unique decoding radius $d/2$, since $d \leq n$.

A simple analysis of (1) shows that

$$\begin{aligned} |\mathrm{Gab}[n,k] \cap B_\tau(c_R)| &\geq \frac{\begin{bmatrix} n/g \\ (n-\tau)/g \end{bmatrix}_{q^g}}{q^{n\ell}} \\ &\geq \frac{(q^g)^{\frac{n-\tau}{g}(\frac{n}{g}-\frac{n-\tau}{g})}}{q^{n\ell}} \\ &= q^{(n-\tau)\frac{\tau}{g}-n\ell} = q^{\frac{n\tau}{g}-\frac{\tau^2}{g}-n\ell} \\ &= q^{n(\ell+1)-g(\ell+1)^2-n\ell} \\ &= q^{n-g(\ell+1)^2} = q^{n-\tau(\ell+1)}, \end{aligned}$$

and hence, this bound results in a list of exponential size whenever $g(\ell+1)^2 < c \cdot n$ for $c \in (0,1)$, or alternatively, when $\tau < \frac{cn}{\ell+1}$.

The following examples provide infinite sets of Gabidulin codes, with rates from $\frac{1}{5}$ to 1, that cannot be list decoded efficiently *at all* according to the bound from Theorem 3. This result strictly outperforms the bound from Corollary 2, and provides an answer to an open problem by [7], [15, Section 6], and [31, Section V], that is, there exist Gabidulin codes that cannot be efficiently list decoded beyond the unique decoding radius.

Example 1. *Let n be an integer power of 2, and let $1 \leq i \leq \log n - 2$. For any integer m such that $n|m$, consider a $\mathrm{Gab}[n, (1-\frac{1}{2^i})n + 2]$ code over $\mathbb{F}_{q^m}$ with evaluation points that span $\beta\mathbb{F}_{q^n}$ for some $\beta \in \mathbb{F}^*_{q^m}$, and let τ be the smallest possible list decoding radius, that is,*

$$\tau \triangleq \left\lfloor \frac{d-1}{2} \right\rfloor + 1 = \left\lfloor \frac{\frac{n}{2^i} - 2}{2} \right\rfloor + 1 = \frac{n}{2^{i+1}}.$$

Let $g \triangleq \frac{n}{2^{i+1}} = \tau$, and notice that $g \geq 2$. To see that $g|\gcd(n, n-\tau)$, notice that since n is an integer power of 2, it follows that $\tau|n$, and thus $g|n$. In addition, we have that $\tau(2^{i+1}-1) = n - \tau$, thus $\tau|(n-\tau)$ and $g|(n-\tau)$. Therefore, in Theorem 3 we may choose $g = \frac{n}{2^{i+1}}, \ell = 0$, and get that there exists a word $c_R \in \mathbb{F}^n_{q^m}$ with $q^{(1-2^{-i-1})n}$ codewords in a ball of radius τ around it. Since τ is larger than the unique decoding radius by one, this code cannot be efficiently list decoded at all. A detailed comparison between this bound and [31] appears in Appendix B.

Example 2. *Let g, α_n, and α_τ be positive integers such that $\alpha_n \geq \alpha_\tau^2 + 1$. For $n = \alpha_n g$, $\tau = \alpha_\tau g$, and any integer m such that $n|m$, consider a $\mathrm{Gab}[n, n - 2\tau + 1]$ code over $\mathbb{F}_{q^m}$ with evaluation points that span $\beta\mathbb{F}_{q^n}$ for some $\beta \in \mathbb{F}^*_{q^m}$, whose minimum distance is $d = 2\tau$, and whose rate is*

$$\frac{n - 2\tau + 1}{n} = 1 - \frac{2\alpha_\tau}{\alpha_n} + \frac{1}{n}.$$

According to Theorem 3, there exists a word c_R having

$$\frac{\begin{bmatrix} n/g \\ (n-\tau)/g \end{bmatrix}_{q^g}}{q^{n\ell}}, \tag{2}$$

codewords in radius τ around it, where $\ell = \tau/g - 1 = \alpha_\tau - 1$. Simplifying this expression, we have that

$$\begin{aligned} \frac{\begin{bmatrix} n/g \\ (n-\tau)/g \end{bmatrix}_{q^g}}{q^{n\ell}} &= \frac{\begin{bmatrix} \alpha_n \\ \alpha_n - \alpha_\tau \end{bmatrix}_{q^g}}{q^{n(\alpha_\tau - 1)}} \\ &\geq \frac{(q^g)^{(\alpha_n - \alpha_\tau)\alpha_\tau}}{q^{n(\alpha_\tau-1)}} \\ &= q^{n - \tau\alpha_\tau} = q^{(\alpha_n - \alpha_\tau^2)g}. \end{aligned}$$

If α_τ and α_n are constants then $g = \Omega(n)$ and $q^{(\alpha_n - \alpha_\tau^2)g} = q^{\Omega(n)}$, which implies that the list size is exponential in the code length. Since $\tau < n/2$, as mentioned after Theorem 3, it follows that $\alpha_n > 2\alpha_\tau$, and thus we have the following two interesting families of codes.

1) *For $\alpha_n = 3$ and $\alpha_\tau = 1$ we have the code $\mathrm{Gab}[3g, g+1]$ over any field $\mathbb{F}_{q^m}$ such that $3g|m$, with evaluation points that span $\beta\mathbb{F}_{q^{3g}}$ for some $\beta \in \mathbb{F}^*_{q^m}$. The rate of this code is $\frac{1}{3} + \frac{1}{n}$, and its minimum distance is $2g$. For the radius $\tau = g$, there exists a word c_R with at least $q^{2g} = q^{\Omega(n)}$ codewords around it, and hence this code cannot be list decoded efficiently at all.*
2) *For $\alpha_n = 5$ and $\alpha_\tau = 2$ we have the code $\mathrm{Gab}[5g, g+1]$ over any field $\mathbb{F}_{q^m}$ such that $5g|m$, with evaluation points that span $\beta\mathbb{F}_{q^{5g}}$ for some $\beta \in \mathbb{F}^*_{q^m}$. The rate of this code is $\frac{1}{5} + \frac{1}{n}$, and its minimum distance is $4g$. For the radius*

$\tau = 2g$, there exists a word c_R with at least $q^g = q^{\Omega(n)}$ codewords around it, and hence this code cannot be list decoded efficiently at all.

Clearly, this strategy can be used to construct examples of families with larger code rates, but $\frac{1}{5} + \frac{1}{n}$ is the smallest one. This may be seen by considering all integers α_τ and α_n which comply with the above constraints. That is, for $\alpha_\tau = 1$ and $\alpha_n \geq 4$, the rate is at least $\frac{1}{2} + \frac{1}{n}$, for $\alpha_\tau = 2$ and $\alpha_n \geq 6$ the rate is at least $\frac{1}{3} + \frac{1}{n}$, and for any $\alpha_\tau \geq 3$ and any $\alpha_n \geq \alpha_\tau^2 + 1$ the rate is at least $\frac{1}{3} + \frac{1}{n}$.

In the following, we present a simple algorithmic way of constructing many dense sets of Gabidulin codewords. These sets also show that the corresponding Gabidulin codes cannot be efficiently list decoded beyond the unique decoding radius. In addition, we have that for certain Gabidulin codes, dense sets of codewords abound and may easily be computed explicitly.

Theorem 4. *Let g, s, n, and m be integers such that $g \geq 2$, $gs|n$, and $n|m$. Let $\mathrm{Gab}[n, n-2gs+1]$ be a linear Gabidulin code over $\mathbb{F}_{q^m}$, with $d = 2gs$ and evaluation points $\alpha_1, \ldots, \alpha_n \in \beta\mathbb{F}_{q^n}$ for some $\beta \in \mathbb{F}_{q^m}^*$. If $\tau \triangleq \lfloor \frac{d-1}{2} \rfloor + 1 = gs$, then there exists an (explicitly defined) word $c_R \in \mathbb{F}_{q^m}^n \setminus \mathrm{Gab}[n, n-2gs+1]$ such that*

$$|\mathrm{Gab}[n, n-2gs+1] \cap B_\tau(c_R)| \geq \frac{q^n - 1}{q^{gs} - 1}.$$

In particular, if R is the polynomial whose evaluation in $\alpha_1, \ldots, \alpha_n$ yields c_R, then $\frac{q^n-1}{q^{gs}-1}$ of the codewords in $B_\tau(c_R)$ are given by the evaluations of $\{R - P_\beta\}_{P_\beta \in \mathcal{Z}_\beta}$ in $\alpha_1, \ldots, \alpha_n$, where $\mathcal{Z}_\beta$ is the set of subspace polynomials which result from shifting $\mathcal{Z}$ (Construction 2) by β.

Proof: Since $gs|n - gs$, by setting $r = n - gs$ it follows from Construction 2 that the set $\mathcal{Z}$ is a set of subspace polynomials of subspaces in $\mathcal{G}_q(n, n-gs)$, whose size is $\frac{q^n-1}{q^{gs}-1}$. Since $n|m$, we have that $\mathbb{F}_{q^n}$ is a subfield of $\mathbb{F}_{q^m}$, and therefore the polynomials in $\mathcal{Z}$ may be considered as polynomials over $\mathbb{F}_{q^m}$ as well. According to Construction 2 and Lemma 6, the polynomials in $\mathcal{Z}$ agree on their topmost gs coefficients $(1, 0, \ldots, 0)$, even when considered as polynomials over $\mathbb{F}_{q^m}$. Similar to the proof of Theorem 3, let $\{V_P\}_{P \in \mathcal{Z}}$ be the set of subspaces in $\mathcal{G}_q(n, n-gs)$ which corresponds to the subspace polyonmials in $\mathcal{Z}$, let P_β denote the subspace polynomial of βV_P, and let $\mathcal{Z}_\beta \triangleq \{P_\beta\}_{P \in \mathcal{Z}}$. Clearly, we have that $|\mathcal{Z}| = |\mathcal{Z}_\beta|$, and by Lemma 1 it follows that the subspace polynomials in $\mathcal{Z}_\beta$ agree of their topmost gs coefficients $(1, 0, \ldots, 0)$.

Let R be any linearized polynomial of q-degree $n - gs$ whose top gs coefficients are $(1, 0, \ldots, 0)$, and let $c_R \in \mathbb{F}_{q^m}^n$ be the word resulting from the evaluation of R at $\alpha_1, \ldots, \alpha_n$. For each $P_\beta \in \mathcal{Z}_\beta$ let $c_{R-P_\beta} \in \mathbb{F}_{q^m}^n$ be the word corresponding to the evaluation of $R - P_\beta$ at $\alpha_1, \ldots, \alpha_n$. For all $P_\beta \in \mathcal{Z}_\beta$ we have that $\deg_q(R - P_\beta) \leq n - 2gs < n - 2gs + 1$, and thus $c_{R-P_\beta} \in \mathrm{Gab}[n, n-2gs+1]$. In addition, $\deg_q R = n - gs$, and thus $c_R \notin \mathrm{Gab}[n, n-2gs+1]$.

As in the proof of Theorem 3, for all $P_\beta \in \mathcal{Z}_\beta$ we have that $\mathrm{rank}(c_R - c_{R-P_\beta}) = \dim P_\beta(\beta\mathbb{F}_{q^n}) = gs$. Therefore, the set $\{c_{R-P_\beta}\}_{P_\beta \in \mathcal{Z}_\beta}$ is a set of $\frac{q^n-1}{q^{gs}-1}$ codewords in $\mathrm{Gab}[n, n-2gs+1]$, all of which are of distance at most $\tau = gs$ from c_R. ■

Notice that each code in the family of codes mentioned in Theorem 4 satisfies $d = 2gs$, and hence the unique decoding radius is $\lfloor \frac{d-1}{2} \rfloor = gs - 1$. Furthermore, since $gs|n$, it follows that $gs \leq \frac{n}{2}$, and thus the word c_R has $\Omega(q^{n/2})$ codewords in a ball of radius $\tau = \lfloor \frac{d-1}{2} \rfloor + 1$ around it. Hence, this family of Gabidulin codes cannot be list decoded efficiently *at all*.

It is an interesting question if our results can be used to derive a lower bound on the number of words that have an exponentially-sized list of codewords around themselves. If it can be proved that there are just a few just words, we might be able to remove a few codewords of the Gabidulin code to obtain a list decodable code of slightly smaller rate. The code constructed in [15] seems to be such a list decodable code.

Further, for *folded* Gabidulin codes such a subcode might be easy to find. The results from [1] show that the *average* list size of folded Gabidulin codes is quite small, indicating that there are only a few words with an exponentially-sized list around them.

Finally, the results in this section can be used to prove bounds for punctured Gabidulin codes, which are obtained by removing coordinates from the original code. Puncturing a $\mathrm{Gab}[n, k]$ code by $s < n - k + 1$ positions yields a $\mathrm{Gab}[n - s, k]$ code. We can therefore provide lower bounds on list decoding of Gabidulin codes where n *does not divide* m.

Lemma 7. *Let $\mathcal{C}$ be a $\mathrm{Gab}[n, k]$ code over $\mathbb{F}_{q^m}$ with minimum distance $d \triangleq n - k + 1$, let s be an integer such that $s < d$, and let $\mathcal{C}_s$ be a $\mathrm{Gab}[n-s, k]$ code which results from $\mathcal{C}$ by s puncturing operations, whose minimum distance is $d' \triangleq n - s - k + 1$. If $\mathcal{C}$ cannot be list decoded efficiently at all, i.e., there exists a word $w \in \mathbb{F}_{q^m}^n$ such that*

$$|\mathcal{C} \cap B_\tau(w)| \geq q^{\Omega(n)}$$

where $\tau \triangleq \lfloor \frac{d-1}{2} \rfloor + 1$, then $\mathcal{C}_s$ cannot be list decoded efficiently for any radius at least $\tau' + s'$, where $\tau' = \lfloor \frac{d'-1}{2} \rfloor + 1$, and

1) *If s is even, then $s' = \frac{s}{2}$.*
2) *If s is odd and $n - k$ is even, then $s' = \frac{s}{2} + \frac{1}{2}$.*
3) *If s and $n - k$ are both odd, then $s' = \frac{s}{2} - \frac{1}{2}$.*

	$\tau = \lfloor \frac{n-k}{2} \rfloor + 1$	$\tau' = \lfloor \frac{n-k-s}{2} \rfloor + 1$	Resulting radius
$n-k$ and s are both even.	$\frac{n-k}{2} + 1$	$\frac{n-k}{2} - \frac{s}{2} + 1$	$\tau = \tau' + \frac{s}{2}$
$n-k$ is odd and s is even.	$\frac{n-k-1}{2} + 1$	$\frac{n-k-1}{2} - \frac{s}{2} + 1$	$\tau = \tau' + \frac{s}{2}$
$n-k$ is even and s is odd.	$\frac{n-k}{2} + 1$	$\frac{n-k}{2} - \frac{s+1}{2} + 1$	$\tau = \tau' + \frac{s}{2} + \frac{1}{2}$
$n-k$ and s are both odd.	$\frac{n-k-1}{2} + 1$	$\frac{n-k-1}{2} - \frac{s-1}{2} + 1$	$\tau = \tau' + \frac{s}{2} - \frac{1}{2}$

TABLE I

THE RESULTING RADIUS IN LEMMA 7. IF $\mathrm{Gab}[n,k]$ CANNOT BE LIST DECODED EFFICIENTLY FOR THE RADIUS τ, THEN THE PUNCTURED CODE $\mathrm{Gab}[n-s,k]$, $s < n-k+1$, CANNOT BE LIST DECODED EFFICIENTLY FOR THIS RADIUS AS WELL. THE RIGHTMOST COLUMN PROVIDES τ AS A FUNCTION OF τ' AND s, WHERE THE UNIQUE DECODING RADIUS OF $\mathrm{Gab}[n-s,k]$ IS $\tau'-1$. THE GIVEN VALUES FOR τ' ARE SIMPLE CALCULATIONS WHICH FOLLOW FROM $n-k-s$ BEING EITHER EVEN OR ODD.

Proof: Since puncturing may only reduce the distance between any two given words, and since any two codewords in $\mathcal{C}$ cannot coincide by puncturing $s < d$ coordinates, it follows that

$$|\mathcal{C}_s \cap B_\tau(w')| \geq q^{\Omega(n)},$$

where $w' \in \mathbb{F}_{q^m}^{n-s}$ is the result of puncturing w. Hence, $\mathcal{C}_s$ cannot be list decoded efficiently beyond the radius τ. Table I presents the values of τ as a function of τ' and s, from which the claim follows. ∎

Since the addition to the unique decoding radius τ' of $\mathrm{Gab}[n-s,k]$ in Lemma 7 is usually nonzero, it is not clear if those punctured codes indeed cannot be list decoded efficiently at *any* radius. However, for the special case where $s=1$ and $n-k$ is odd, we obtain the following corollary.

Corollary 3. *For integers $0 < k < n$ such that $n-k$ is odd, if $\mathrm{Gab}[n,k]$ cannot be list decoded efficiently at all, i.e., there exist a word $w \in \mathbb{F}_{q^m}^n$ such that*

$$|\mathcal{C} \cap B_\tau(w)| \geq q^{\Omega(n)}$$

where $\tau \triangleq \lfloor \frac{d-1}{2} \rfloor + 1$, then the punctured code $\mathrm{Gab}[n-1,k]$ cannot be list decoded efficiently at all.

Although Corollary 3 does not provide a drastic improvement in the variety of codes to which our bounds apply, it does imply the important observation that the divisibility constraints between n and m in Theorem 3 and Theorem 4 *are not necessary*. In addition, one may obtain infinite examples of Corollary 3 by puncturing either of the codes $\mathrm{Gab}[3g, g+1]$ and $\mathrm{Gab}[5g, g+1]$ from Example 2, and thus obtain $\mathrm{Gab}[3g-1, g+1]$ and $\mathrm{Gab}[5g-1, g+1]$ codes that cannot be list decoded efficiently at all.

V. BOUNDS FOR CONSTANT-DIMENSION SUBSPACE CODES

In this section, we state new bounds on list decoding *lifted Gabidulin codes* (see [30]), which are a class of almost-optimal constant dimension subspace codes. Lifted Gabidulin codes are of special interest since, in contrast to many other subspace code constructions, they can be efficiently decoded (see [30]) while only losing a relatively small number of codewords compared to other subspace code constructions. These bounds are a direct consequence of our bounds for list decoding Gabidulin codes (Theorem 3 and Theorem 4).

Throughout this section, the quadruple $(n, M_s, d_s, r)_q$ denotes a constant dimension subspace code in the Grassmannian $\mathcal{G}_q(n,r)$ of cardinality M_s and minimum subspace distance d_s. Further, $\langle A \rangle$ denotes the subspace spanned by the rows of a matrix A. The *lifting* is a map which is applied to a single matrix or a set of matrices and is defined as follows.

Definition 4. *Consider the mapping*

$$\begin{aligned} \mathcal{I}: \quad \mathbb{F}_q^{n\times m} &\to \mathcal{G}_q(n, n+m) \\ X &\mapsto \langle [I_n \ X] \rangle, \end{aligned}$$

where I_n denotes the $n \times n$ identity matrix. The subspace $\mathcal{I}(X) = \langle [I_n \ X] \rangle$ is called lifting of the matrix X. If we apply this map on all codewords of a code $\mathcal{C}$ (in matrix representation), then the subspace code $\mathcal{I}(\mathcal{C})$ is called lifting of the code C.

The properties of a lifted code were studied by Silva, Kschischang and Kötter and are summarized in the following two lemmas.

Lemma 8. *[30] Let $X, Y \in \mathbb{F}_q^{n\times m}$ and let $\mathcal{I}(X), \mathcal{I}(Y) \in \mathcal{G}_q(n+m, n)$ be as in Definition 4. Then,*

$$d_s(\mathcal{I}(X), \mathcal{I}(Y)) = 2 \cdot d_R(X,Y).$$

Proof:

$$\begin{aligned} d_s\left(\mathcal{I}\left(X\right),\mathcal{I}\left(Y\right)\right) &= 2\dim\left(\mathcal{I}\left(X\right)+\mathcal{I}\left(Y\right)\right) \\ &\quad -\dim\left(\mathcal{I}\left(X\right)\right)-\dim\left(\mathcal{I}\left(Y\right)\right) \\ &= 2\,\mathrm{rank}\begin{pmatrix} I_n & X \\ I_n & Y \end{pmatrix} - 2n \\ &= 2\,\mathrm{rank}\begin{pmatrix} I_n & X \\ \mathbf{0} & Y-X \end{pmatrix} - 2n \\ &= 2\left[\mathrm{rank}(I_n)+\mathrm{rank}(X-Y)\right]-2n \\ &= 2\,\mathrm{rank}(X-Y) = 2d_R(X,Y). \end{aligned}$$

■

The following lemma directly follows from Lemma 8.

Lemma 9. *[30] Let $\mathcal{C}$ be a rank-metric code over $\mathbb{F}_{q^m}$ of length $n \leq m$, minimum rank distance d_R and cardinality M_R, whose codewords are represented as $m \times n$ matrices over $\mathbb{F}_q$. Then, the lifting of the transposed codewords, i.e.,*

$$\mathcal{I}\left(\mathcal{C}^T\right) \triangleq \left\{\mathcal{I}\left(C^T\right) = \left\langle [I_n \; C^T] \right\rangle \;\middle|\; C \in \mathcal{C}\right\}$$

is an $(n+m, M_s = M_R, d_s = 2d_R, n)_q$ constant dimension subspace code.

Hence, the lifting of the transpose of a $\mathrm{Gab}[n,k]$ code over $\mathbb{F}_{q^m}$ with $n \leq m$, minimum rank distance $d = n-k+1$ and cardinality $M_R = q^{mk}$ results in an $(n+m, q^{mk}, 2d, n)_q$ constant dimension subspace code in the Grassmannian $\mathcal{G}_q\left(n+m, m\right)$.

So far, the only known bound to list decoding subspace codes was given in [26] and is based on the results for Gabidulin codes from [31]. The following theorem summarizes the result from [26].

Theorem 5. *[26, Theorem 37] Let $\mathcal{C}$ be a linear $\mathrm{Gab}[n,k]$ Gabidulin code over $\mathbb{F}_{q^m}$ of length $n \leq m$, $d = n-k+1$, evaluation points $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{q^m}$, and let τ be an integer such that $\lfloor \tau/2 \rfloor < d$. Denote by $\mathcal{I}\left(\mathcal{C}^T\right)$ the $(n+m, q^{mk}, 2d, n)_q$ subspace code from the lifting of the code $\mathcal{C}$ as in Definition 4. Then, there is a subspace $\langle R \rangle$ such that*

$$\left|\mathcal{I}\left(\mathcal{C}^T\right) \cap B_\tau^s(\langle R \rangle)\right| \geq \frac{\begin{bmatrix} n \\ \lfloor \tau/2 \rfloor \end{bmatrix}_q}{q^{m(n-k-\lfloor \tau/2 \rfloor)}}.$$

Let $B_\tau^s(\langle W \rangle) \triangleq \{\langle V \rangle \mid d_s(\langle W \rangle, \langle V \rangle) \leq \tau\}$ denote a ball of radius τ centered at $\langle W \rangle$ in the subspace distance. With Lemma 8, we obtain the following relation between a rank-metric code $\mathcal{C}$ and its lifted subspace code $\mathcal{I}\left(\mathcal{C}^T\right)$:

$$|\,\mathcal{C} \cap B_\tau(c_R)| \leq \left|\mathcal{I}\left(\mathcal{C}^T\right) \cap B_{2\tau}^s(\mathcal{I}\left(c_R^T\right))\right|. \tag{3}$$

This relation and Theorem 3 provide the following theorem on the list size of lifted Gabidulin codes.

Theorem 6. *Let $\mathcal{C}$ be a linear $\mathrm{Gab}[n,k]$ Gabidulin code over $\mathbb{F}_{q^m}$ with length $n \mid m$, $d = n-k+1$, and evaluation points $\alpha_1, \ldots, \alpha_n \in \beta\mathbb{F}_{q^n}$ for some $\beta \in \mathbb{F}_{q^m}^*$. Let τ, g be integers such that $\lfloor \frac{d-1}{2} \rfloor + 1 \leq \lfloor \frac{\tau}{2} \rfloor \leq d-1$, $g \geq 2$, and $g \mid \gcd(n - \lfloor \frac{\tau}{2} \rfloor, n)$. Let ℓ be the unique integer such that $n = n - \lfloor \frac{\tau}{2} \rfloor + g(\ell+1)$ (and thus, $\lfloor \frac{\tau}{2} \rfloor = g(\ell+1)$) and denote by $\mathcal{I}\left(\mathcal{C}^T\right)$ the $(n+m, q^{mk}, 2d, n)_q$ subspace code from the lifting of the code $\mathcal{C}$ as in Definition 4.*

Then there exists a subspace $\mathcal{I}\left(c_R^T\right) \in \mathcal{G}_q\left(n+m, n\right)$, where $c_R \in \mathbb{F}_{q^m}^n \setminus \mathrm{Gab}[n,k]$ such that

$$\begin{aligned} \left|\mathcal{I}\left(\mathcal{C}^T\right) \cap B_\tau^s(\mathcal{I}\left(c_R^T\right))\right| &\geq \frac{\begin{bmatrix} n/g \\ (n-\lfloor \tau/2 \rfloor)/g \end{bmatrix}_{q^g}}{q^{n\ell}} \\ &\geq q^{n-\lfloor \tau/2 \rfloor(\ell+1)}. \end{aligned}$$

Proof: The statement follows from (3) and Theorem 3. The floor operation for $\lfloor \tau/2 \rfloor$ is necessary since the subspace distance is an even number, see explanation of the proof of [26, Theorem 37]. ■

Thus, this bound results in a list of exponential size for even τ when $\tau < \frac{2cn}{\ell+1}$ and for odd τ when $\tau < \frac{2cn}{\ell+1} + 1$ for $c \in (0,1)$, which results for many cases in a better bound than the one from [26, Theorem 37]. Similarly, from Theorem 4, we obtain the following theorem.

Theorem 7. *Let g, s, n, and m be integers such that $g \geq 2$, $gs|n$, and $n|m$. Let $\mathcal{C}$ be a linear $\mathrm{Gab}[n, n-2gs+1]$ Gabidulin code over $\mathbb{F}_{q^m}$, with $d = 2gs$ and evaluation points $\alpha_1, \ldots, \alpha_n \in \beta\mathbb{F}_{q^n}$ for some $\beta \in \mathbb{F}_{q^m}^*$. Denote by $\mathcal{I}\left(\mathcal{C}^T\right)$ the $(n+m, q^{m(n-2gs+1)}, 2d, n)_q$ subspace code from the lifting of the code $\mathcal{C}$ as in Definition 4.*

If $\lfloor \frac{\tau}{2} \rfloor \triangleq \lfloor \frac{d-1}{2} \rfloor + 1 = gs$, then there exists an (explicitly defined) subspace $\mathcal{I}\left(c_R^T\right) \in \mathcal{G}_q\left(n+m, n\right)$, where

$$c_R \in \mathbb{F}_{q^m}^n \setminus \mathrm{Gab}[n, n-2gs+1],$$

such that

$$\left|\mathcal{I}\left(\mathcal{C}^T\right) \cap B_\tau^s(\mathcal{I}\left(c_R^T\right))\right| \geq \frac{q^n-1}{q^{gs}-1} = \frac{q^n-1}{q^{\lfloor \tau/2 \rfloor}-1}.$$

The explicitly defined subspace follows directly from lifting the matrix representation of the explicit word of Theorem 4. In [31], a non-linear rank-metric code was presented which cannot be list decoded efficiently at all. The lifting of this code obviously results in a subspace code with the same restrictions to list decoding as lifted Gabidulin codes. However, lifted Gabidulin codes are of special interest for network coding and therefore, we have analyzed their list decoding capability in this section.

VI. Conclusions and Future Work

We have improved the worst-case bound on the list decodability of Gabidulin codes in many cases. This was shown by using the structure of the subspace polynomials of a subset of $\mathcal{G}_q(n,r)$ for n and r that have a non-trivial $\gcd$. In addition, we have presented such subspace polynomials explicitly, using the notions of cyclic shifts and q-associativity. Both of these results outperform the counting argument applied in [31], and provide examples of infinite families of Gabidulin codes that cannot be list decoded efficiently beyond the unique decoding radius. This resolves an open question by [7], [15], and [31] and reveals a significant difference between decoding Gabidulin and Reed–Solomon codes despite their similar code definitions.

The work of [31] ruled out the existence of an efficient algorithm for list decoding of Gabidulin codes beyond the Johnson radius. Our work rules out the existence of an efficient list decoding algorithm that applies for any Gabidulin code and any radius beyond half the minimum distance. However, this certainly does not rule out the existence of an efficient algorithm for list decoding of very large subcodes of Gabidulin codes or Gabidulin codes with lower rates, since our work requires the code parameters to satisfy some strict number-theoretic and field-theoretic constraints, and our examples have rate at least $\frac{1}{5}$. For example, [15] provides a subcode of a Gabidulin code which can be list decoded efficiently.

We have also shown that identical results hold for lifted Gabidulin codes, which are an important class of nearly optimal subspace codes. Additional discussion about the inapplicability of our techniques to improve the known combinatorial bound on list decoding of Reed–Solomon codes appears in Appendix A.

For future research, we would like to have similar bounds on Gabidulin codes in $\mathbb{F}_{q^m}^n$ where the evaluation points do not necessarily come from a cyclic shift of $\mathbb{F}_{q^n}$. This seems to require a rigorous understanding of the connection between the subspace polynomials of a given subspace V and the subspace $A \cdot V$, where A is a nonsingular transform. Moreover, we would like to generalize our results for *any* case where n does not necessarily divide m, a problem which seems to require generalizing Lemma 6 to the case $n \nmid m$. In addition, we would like to derive bounds for Gabidulin codes with rates less than $\frac{1}{5}$.

Appendix A

In [4], limits for list decoding of Reed–Solomon codes were shown using techniques which highly resemble the ones in [31] and in this paper. The interested reader might conjecture that the improvement achieved here (see Theorem 3 and Theorem 4) for Gabidulin codes may also be attained for Reed–Solomon codes, for which list decoding related problems were very extensively studied. In what follows we briefly describe why such an improvement cannot be directly attained by our techniques. Adapting these techniques to Reed–Solomon codes remains an intriguing open problem. In the sequel, we briefly describe the methods and results of [4].

Following the notations in [4], a Reed–Solomon code $\mathrm{RS}[q^n, q^u]$ of length q^n and dimension q^u is a subset of $\mathbb{F}_{q^n}^{q^n}$ such that

$$\mathrm{RS}[q^n, q^u] \triangleq \left\{ (p(\alpha_1), \ldots, p(\alpha_{q^n})) \;\middle|\; \begin{array}{c} p : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n} \text{ is a} \\ \text{polynomial with} \\ \deg(p) < q^u \end{array} \right\},$$

where $\{\alpha_i\}_{i=1}^{q^n}$ are *all* elements of $\mathbb{F}_{q^n}$. Notice that Reed–Solomon codes may be defined as the evaluation of polynomials in any number of elements in the field. However, we consider this definition for convenience. Notice also that any word $w \in \mathbb{F}_{q^n}^{q^n}$ may be regarded as a polynomial over $\mathbb{F}_{q^n}$, and any word $c \in \mathrm{RS}[q^n, q^u]$ may be regarded as a polynomial over $\mathbb{F}_{q^n}$ of *bounded degree*.

Definition 5. *[4, Definition 3.3] A family of polynomials $\mathcal{P} \subseteq \mathbb{F}_{q^n}[x]$ is said to be an (a,s)-family if*

1) *Each polynomial in $\mathcal{P}$ has at least a roots in $\mathbb{F}_{q^n}$.*
2) *There is a polynomial P^* such that for all $P \in \mathcal{P}$, $P^* - P$ has degree at most s. We refer to P^* as a pivot of the family.*

Lemma 10. *[4, Proposition 3.5] Let a, s and ℓ be positive integers. Then, the following are equivalent.*

1) *There is a word $w : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ and ℓ polynomials $P_1, \ldots, P_\ell$ of degree at most s such that for $i = 1, 2, \ldots, \ell$, P_i and w agree on at least a points of $\mathbb{F}_{q^n}$.*
2) *There is an (a,s)-family of size ℓ of polynomials, whose pivot is the unique polynomial P_w that agrees with the word w on all elements in $\mathbb{F}_{q^n}$.*

The polynomial P_w corresponds to the "problematic" word, that is, the word that has exponentially many codewords in a small radius around it. The polynomials $P_1, \ldots, P_\ell$, having a low degree, are the codewords surrounding P_w. It is readily verified that the polynomials $P_1, \ldots, P_\ell$ are inside a ball of small radius centered at P_w if and only if the polynomials $\{P_w - P_i\}_{i=1}^{s}$ have multiple roots in $\mathbb{F}_{q^n}$. As subspace polynomials have many roots over $\mathbb{F}_{q^n}$, they are good candidates for playing the role of the polynomials $\{P_w - P_i\}_{i=1}^{s}$. This intuition is formalized as follows.

Lemma 11. *[4] If $S \subseteq \mathcal{G}_q(n, r)$ is a set of subspaces whose corresponding subspace polynomials have identical $r - t$ top coefficients for some integer $t < r$, then the set of subspace polynomials of S forms a (q^r, q^t)-family.*

Proof: Let W be the set of subspace polynomials of the subspace in the set S. Since every polynomial in W is a subspace polynomial, it has exactly q^r roots in $\mathbb{F}_{q^n}$. If P_w is the linearized polynomial consisting of the $r - t$ mutual top coefficients of the polynomials in W, then $\deg(P_w - P_i) \leq q^t$ for all $P_i \in W$. ∎

In light of Lemma 10 and Lemma 11, presenting a large family of subspace polynomials that agree on many top coefficients suffices for providing a word that is adjacent to too many Reed–Solomon codewords. Such a family of size $\begin{bmatrix} n/g \\ r/g \end{bmatrix}_{q^g} / q^{n\ell}$ was presented in Theorem 1, where $g | \gcd(n, r)$ and $\ell = \frac{n-r}{g} - 1$. Using the standard bound on the Gaussian coefficient (see Section I) we have that

$$\frac{\begin{bmatrix} n/g \\ r/g \end{bmatrix}_{q^g}}{q^{n\ell}} \leq 4q^{\frac{r}{g}(n-r)-n\ell}.$$

Plugging in the expression for ℓ results in an upper bound of $4q^n$, and hence the size of the family is not more than 4 times the length of the code, which is q^n. In addition, an explicit family can be derived from Construction 2 whose size is not super-polynomial in n either, and hence a super-polynomial list decoding bound is *not* achieved.

Both of these families do provide dense sets that are larger than the ones achieved by a counting argument. Dense sets of Reed–Solomon codewords have applications in hardness of approximating the minimum distance of a linear code [8] and in constructing error-correcting codes with improved parameters [32]. However, the dense sets provided by our results are not nearly large enough for these applications.

APPENDIX B

The following lemmas shows that the bound from Theorem 3 strictly outperforms the bound implied by Theorem 2 and Corollary 2, given in [31], when applied over the code in Example 1.

Lemma 12. *For any $i \geq 1$,*

$$1 - \sqrt{\frac{2^i - 1}{2^i}} > \frac{1}{2^{i+1}}.$$

Proof: Clearly, $\frac{1}{2^{i+2}} > 0$, and hence,

$$\begin{aligned}
2^i - 1 + \frac{1}{2^{i+2}} &> 2^i - 1 \\
1 - \frac{2}{2^{i+1}} + \frac{1}{2^{2i+2}} &> \frac{2^i - 1}{2^i} \\
\left(1 - \frac{1}{2^{i+1}}\right)^2 &> \frac{2^i - 1}{2^i} \\
1 - \frac{1}{2^{i+1}} &> \sqrt{\frac{2^i - 1}{2^i}} \\
1 - \sqrt{\frac{2^i - 1}{2^i}} &> \frac{1}{2^{i+1}}
\end{aligned}$$

∎

Lemma 13. *For a large enough n, the radius $\tau = \frac{n}{2^{i+1}}$, for which the code in Example 1 cannot be list decoded efficiently according to Theorem 3, is strictly smaller than the radius τ' which is guaranteed by the Corollary 2.*

Proof: Inserting $\varepsilon = 1$ into the bound of Corollary 2 provides a stronger bound than Corollary 2 for any $\varepsilon < 1$. Therefore, when our bound outperforms Corollary 2 with $\varepsilon = 1$, our bound also outperforms Corollary 2 with $\varepsilon < 1$.

Since in Example 1 we have $d = \frac{n}{2^i} - 1$ it follows that

$$\begin{aligned} \tau' &\geq \frac{m+n}{2} - \sqrt{\frac{(m+n)^2}{4} - m(d-1)} \\ &= \frac{m+n}{2} - \sqrt{\frac{(m+n)^2}{4} - m\left(\frac{n}{2^i} - 2\right)} \\ &= \left(\frac{m+n}{2}\right)\left(1 - \sqrt{1 - \frac{4m(d-1)}{(m+n)^2}}\right). \end{aligned} \tag{4}$$

Notice that by Theorem 2, the bound of [31] is weaker if $m > n$, whereas the bound of Theorem 3 does not depend on m. Therefore, it suffices to show that the bound from Theorem 3 outperforms the one from [31] for $m = n$. In this case, (4) simplifies to

$$\tau' \geq n\left(1 - \sqrt{1 - \frac{1}{2^i} + \frac{2}{n}}\right). \tag{5}$$

For a large enough n the term $\frac{2}{n}$ may be neglected. Hence, by Lemma 12, (5) implies that

$$\tau' \geq n\left(1 - \sqrt{\frac{2^i - 1}{2^i}}\right) > \frac{n}{2^{i+1}} = \tau.$$

■

ACKNOWLEDGMENT

The authors would like to thank Ron M. Roth for bringing up the idea of puncturing Gabidulin codes (Lemma 7 and Corollary 3), and the idea of Example 2. The authors would also like to thank the reviewers whose comments helped to improve the presentation of the paper, and finally, to Pierre Loidreau, for pointing out an error in previous versions of this paper.

REFERENCES

[1] H. Bartz and V. Sidorenko, "List and Probabilistic Unique Decoding of Folded Subspace Codes," *IEEE International Symposium on Information Theory (ISIT)*, pp. 11–15, 2015.
[2] E. Ben-Sasson, T. Etzion, A. Gabizon, and N. Raviv, "Subspace polynomials and cyclic subspace codes," *IEEE Transactions on Information Theory*, vol. 62, no. 1, pp. 1–9, 2016.
[3] E. Ben-Sasson and S. Kopparty, "Affine dispersers from subspace polynomials," *SIAM Journal on Computing*, vol. 41, no. 4, pp. 880–914, 2012.
[4] E. Ben-Sasson, S. Kopparty, and J. Radhakrishnan, "Subspace polynomials and limits to list decoding of Reed Solomon-codes," *IEEE Transactions on Information Theory*, vol. 56, no. 1, pp. 113–120, 2010.
[5] Q. Cheng, S. Gao, and D. Wan, "Constructing high order elements through subspace polynomials," *Symposium on Discrete Algorithms (SODA)*, pp. 1457–1463, 2012.
[6] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory," *Journal of Combinatorial Theory*, Series A, vol. 25, no. 3, pp. 226–241, 1978.
[7] Y. Ding, "On list decodability of random rank metric codes and subspace codes." *IEEE Transactions on Information Theory*, vol. 61, no.1, pp.51–59, 2015.
[8] I. Dumer, D. Micciancio, and M. Sudan, "Hardness of approximating the minimum distance of a linear code," *IEEE Transactions on Information Theory*, vol. 49, no. 1, pp. 22–37, 2003.
[9] T. Etzion and A. Vardy, "Error-correcting codes in projective space," *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 1165–1173, 2011.
[10] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problems of Information Transmission (English translation of Problemy Peredachi Informatsii)*, vol. 21, 1985.
[11] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov, "Ideals over a noncommutative ring and their applications to cryptography," *Eurocrypt*, pp. 482-489, 1991.
[12] M. Gadouleau and Z. Yan, "Constant-rank codes and their connection to constant-dimension codes," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3207–3216, 2010.
[13] V. Guruswami, *Algorithmic results in list decoding*, Now Publishers Inc, 2006.
[14] V. Guruswami and M. Sudan, "Improved decoding of Reed–Solomon and Algebraic–Geometry Codes," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 1757–1767, Sep. 1999.
[15] V. Guruswami and C. Wang, "Evading subspaces over large fields and explicit list decodable rank-metric codes," *APPROX-RANDOM*, pp. 748-761, 2014.
[16] V. Guruswami, S. Narayanan, and C. Wang, "List decoding subspace codes from insertions and deletions,", *Innovations in Theoretical Computer Science (ITCS)*, pp. 183–189, 2012.
[17] R. Kötter and F.R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3579–3591, 2008.
[18] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20 of *Encyclopedia of Mathematics and Its Applications*. Cambridge University Press, 1997.
[19] P. Loidreau, "Designing a rank metric based McEliece cryptosystem," *Post-Quantum Cryptography*, pp. 142–152, 2010.
[20] P. Lusina, E. M. Gabidulin, and M. Bossert, "Maximum rank distance codes as space-time codes," *IEEE Transactions on Information Theory*, vol. 49, no. 10, pp. 2757–2760, 2003.
[21] H. F. Lu and P. V. Kumar, "Generalized unified construction of space-time codes with optimal rate-diversity tradeoff," *IEEE International Symposium on Information Theory (ISIT)*, p. 95–99, 2004.

[22] H. Mahdavifar and A. Vardy, “Algebraic list decoding of subspace codes,” *IEEE Transactions on Information Theory*, vol. 59, no. 12, pp. 7814–7828, 2013.
[23] H. Mahdavifar and A. Vardy, “Algebraic list decoding of subspace codes with multiplicities,” *49th Annual Allerton Conference on Communication, Control, and Computing*, pp. 1430–1437, 2011.
[24] Ø. Ore, “On a special class of polynomials,” *Transactions of the American Mathematical Society*, vol. 35, no. 3, pp. 559–584, 1933.
[25] N. Raviv and A. Wachter-Zeh, “Some Gabidulin codes cannot be list decoded efficiently at any radius,” *IEEE International Symposium on Information Theory (ISIT)*, pp.6–10, 2015.
[26] J. Rosenthal, N. Silberstein, and A.-L. Trautmann, “On the geometry of balls in the Grassmannian and list decoding of lifted Gabidulin codes,” *Designs, Codes and Cryptography*, vol. 73, no. 2, pp. 393–416, 2014.
[27] R. Roth, “Maximum-rank array codes and their application to crisscross error correction,” *IEEE Transaction on Information Theory*, vol. 37, pp. 328–336, 2006.
[28] N. Silberstein, A. S. Rawat, O. O. Koyluoglu, and S. Vishwanath, “Optimal locally repairable codes via rank-metric codes,” *IEEE International Symposium on Information Theory (ISIT)*, pp. 1819–1823, 2013.
[29] N. Silberstein, A. S. Rawat, and S. Vishwanath, “Error resilience in distributed storage via rank-metric codes,” *Allerton Conference on Communication, Control, Computing*, pp. 1150–1157, 2012.
[30] D. Silva, F. Kschischang, and R. Kötter, “A rank-metric approach to error control in random network coding,” *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 3951–3967, 2008.
[31] A. Wachter-Zeh, “Bounds on list decoding of rank-metric codes,” *IEEE Transactions on Information Theory*, vol. 59, no. 11, pp. 7268–7277, 2013.
[32] C. Xing, “Nonlinear codes from algebraic curves improving the Tsfasman-Vladut-Zink bound,” *IEEE Transactions on Information Theory*, vol. 49, no. 7, pp. 1653–1657, 2003.

Netanel Raviv (S’15) received a B.Sc. degree from the department of mathematics and an M.Sc. degree from the department of Computer Science at the Technion–Israel Institute of Technology, Haifa, Israel, at 2010 and 2013, respectively. He is now a Doctoral student at the department of Computer Science at the Technion. He is an awardee of the IBM Ph.D. fellowship for the academic year of 2015-2016, and the Aharon and Ephraim Katzir study grant for 2015. His research interests include coding for distributed storage systems, algebraic coding theory, network coding, and algebraic structures.

Antonia Wachter-Zeh (S’10–M’14) received a B.S. degree in electrical engineering in 2007 from the University of Applied Science Ravensburg, Germany, and the M.S. degree in communications technology in 2009 from Ulm University, Germany. She obtained her Ph.D. degree in 2013 at the Institute of Communications Engineering, University of Ulm, Germany and at the Institut de recherche mathmatique de Rennes (IRMAR), Universit de Rennes 1, Rennes, France. Currently, she is a postdoctoral researcher at the Technion—Israel Institute of Technology, Haifa, Israel. Her research interests are coding and information theory and their applications.